DOCID: 4165204

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

12 September 2008

MEMORANDUM FOR THE CHAIRMAN, INTELLIGENCE OVERSIGHT BOARD

THRU: Assistant to the Secretary of Defense (Intelligence Oversight)

SUBJECT: (U//~~FOUO~~) Report to the Intelligence Oversight Board on NSA Activities - INFORMATION MEMORANDUM

(U//~~FOUO~~) Except as previously reported to you or the President, or otherwise stated in the enclosure, we have no reason to believe that any intelligence activities of the National Security Agency during the quarter ending 30 June 2008 were unlawful or contrary to Executive Order or Presidential Directive and thus should have been reported pursuant to Section 1.7.(d) of Executive Order 12333.

(U//~~FOUO~~) The Inspector General and the General Counsel continue to exercise oversight of Agency activities by inspections, surveys, training, review of directives and guidelines, and advice and counsel. These activities and other data requested by the Board or members of the staff of the Assistant to the Secretary of Defense (Intelligence Oversight) are described in the enclosure.

George Ellard

GEORGE ELLARD
Inspector General

VITO T. POTENZA
General Counsel

(U//~~FOUO~~) I concur in the report of the Inspector General and the General Counsel and hereby make it our combined report.

KEITH B. ALEXANDER
Lieutenant General, U. S. Army
Director, NSA/Chief, CSS

Encl:
Quarterly Report

This document may be declassified and marked "UNCLASSIFIED/~~For Official Use Only~~" upon removal of enclosure(s)

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

Approved for Release by NSA on 12-19-2014, FOIA Case # 70809 (Litigation)

1. (U//~~FOUO~~) Intelligence, counterintelligence, and intelligence-related activities that violate law, regulation, or policy substantiated during the quarter, as well as actions taken as a result of the violations.

(U) **Intelligence Activities**

(b) (1)
(b) (3)-P.L. 86-36

~~(TS//SI// REL TO USA, FVEY)~~ **Unintentional collection against United States persons.** This quarter, there were [ ] instances in which Signals Intelligence (SIGINT) analysts inadvertently collected communications to, from, or about U. S. persons while pursuing foreign intelligence tasking. All intercepts and reports have been deleted or destroyed as required by United States SIGINT Directive (USSID) SP0018.

(U) Unauthorized Targeting

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 3024(i)

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)

(b) (1)
(b) (3)-P.L. 86-36

~~(TS//SI//NF)~~ An NSA/CSS analyst tasked the telephone numbers associated with a U.S. [ ] without verifying that consent for collection had been given by the person and approved by DIRNSA. The selectors, on coverage from [ ] were detasked. [ ] intercepts were purged from data repositories [ ] when the mistake was found during a target review.

~~(TS//SI//NF)~~ [ ]

(b) (1)
(b) (3)-P.L. 86-36

~~(S//SI//NF)~~ [ ] an NSA/CSS [ ] analyst targeted a foreign person in the United States without Attorney General authorization. She learned that a person tied to the [ ] was in the United States and was suspected to have planned an operation to take place [ ] Thinking only of the urgency and not the target's location, the analyst queried an NSA database for information without seeking authorization to target the individual. No results were returned. The incident was found by the analyst's auditor, and the analyst was counseled and received remedial training.

~~(TS//SI//NF)~~ An oversight resulted in the continued targeting of a U.S. person after his consent to monitoring expired. [ ] Although the consent expired on [ ] NSA/CSS analysts did not remove the selector from collection until [ ] There were [ ] intercepts that were purged from NSA databases.

~~(TS//SI//NF)~~ An NSA/CSS analyst tasked collection on a U.S. person before receiving Attorney General authorization on [ ] The analyst wrongly believed that authorization had been received. The unauthorized action resulted in the intercept of [ ]

(b) (1)
(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-18 USC 798

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

(b)(1)
(b)(3)-P.L. 86-36

between [redacted]. All collected data was purged when the violation was discovered [redacted] and no reports were issued on the data.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

(U) Computer Network Exploitation (CNE)

~~(TS//SI//REL TO USA, FVEY)~~ [redacted]

(U) Database Queries

(b)(1)
(b)(3)-P.L. 86-36

~~(S//SI//REL TO USA, FVEY)~~ There were [redacted] instances of unintentional collection resulting from poorly constructed database queries. All results were deleted from the [redacted] system.

(U) U.S. Person Status

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ On [redacted] occasions, targets initially thought to be legitimate and foreign were found to hold U.S. citizenship. [redacted] NSA terminated targeting [redacted] when the [redacted] relayed that the target held a U.S. passport. Collection was purged from databases, and [redacted] reports were cancelled. [redacted] selector was not detasked when U.S. person status was suspected. The detasking failure resulted in [redacted] intercepts between [redacted], when the selectors were positively linked to an [redacted] The selectors were detasked, collection was purged [redacted] and NSA/CSS analysts were retrained on the process for vetting inadvertent collection.

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ [redacted] NSA/CSS analysts targeted U.S. persons. [redacted] the analyst searched for a U.S. [redacted] a raw traffic database because he did not realize that the [redacted] was owned by a U.S. company. [redacted] the analyst did not follow research procedures, which required him to check [redacted] occurred when another analyst failed to review [redacted] Queries were terminated, and results were not retained. [redacted] mistakes were found during the auditing and oversight functions, and the analysts were retrained on search procedures.

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ Collection transcription [redacted] revealed that a [redacted] was used by a U.S. Government employee on [redacted]. The transcript noted a conversation between two U.S. Government employees. When NSA/CSS learned of the incidental collection, minimization procedures were applied as directed by the USSID SP0018.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

~~(S//SI//REL TO USA, FVEY)~~ a valid foreign target the United States. Tasking was terminated, and collection was purged from NSA databases. No reports were issued.

(b)(1)
(b)(3)-P.L. 86-36

(U) Detasking Delays

~~(TS//SI//REL TO USA, FVEY)~~ the United States on selectors attributed to a target were detasked on however, did not detask Research is ongoing to isolate the cause of the problem, The intercept associated with the the United States was purged from NSA databases

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(b)(1)
(b)(3)-P.L. 86-36

(U//~~FOUO~~) Foreign Intelligence Surveillance Court (FISC)-Authorized Collection

~~(TS//SI//NF)~~ an NSA/CSS analyst discovered a FISC-authorized selector associated with a foreign had not been removed from tasking Pursuant to the FISC order, detasking However, a problem with the collection system prevented the execution of the action. When the system problem was rectified a review of target selectors was conducted. additional selectors affected by the system problem were removed from tasking.

~~(S//SI//REL TO USA, FVEY)~~ **Unintentional dissemination of U.S. identities.** There were instances in which SIGINT analysts disseminated communications to, from, or about U.S. persons while pursuing foreign intelligence tasking this quarter. All data have been deleted or destroyed as required by USSID SP0018.

(b)(1)
(b)(3)-P.L. 86-36

~~(S//SI//REL TO USA, FVEY)~~ During this quarter, SIGINT products were cancelled because they contained the identities of U.S. persons, organizations, or entities. In all instances, the reports were either not reissued or were reissued with proper minimization.

(b)(1)
(b)(3)-P.L. 86-36

~~(S//NF)~~ information about a U.S. person was posted on INTELINK, which is a classified and highly secure intranet used by the U.S. Intelligence Community. A graphic containing a U.S. address was posted when the mistake was identified and corrected.

~~(TS//SI//NF)~~ during a review of intercept an NSA/CSS analyst discovered that the from a legitimate foreign target in the United States from was notified and destroyed the intercepts for the timeframe the target was in the United States.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

(U//~~FOUO~~) Dissemination of Foreign Intelligence Surveillance Court (FISC)-Authorized Collection

~~(TS//SI//NF)~~ an NSA/CSS analyst tipped information on intercepts to other SIGINT analysts using a communication

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

tool that was not authorized as a dissemination tool for [redacted] data because the chat tool does not have the ability to track U.S. person information. When recognized [redacted] the data was deleted. Although not a violation of the FISA and related authorities, the practice does not provide an audit trail of the U.S. person information passed to others within the SIGINT production chain. The process for using the chat tool was amended [redacted]

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ The identity of a U.S. person was not masked [redacted] when a file on a FISC-authorized target [redacted] The [redacted] analyst recognized the oversight, deleted the file and notified NSA. The NSA/CSS analysts associated with the violation were retrained on FISA minimization.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(U) The Protect America Act of 2007 (PAA)

(b)(1)
(b)(3)-P.L. 86-36

~~(S//SI//NF)~~ On [redacted] occasions, NSA/CSS analysts did not purge PAA-related collection from NSA databases in a timely manner. [redacted] an email selector of a legitimate foreign target was detasked because [redacted] Although the database purging began [redacted] collection from the [redacted] databases was not removed until [redacted], another target selector was detasked, but the purging of [redacted] databases was not completed until [redacted] Lastly, [redacted] a target selector was detasked, but the data was not completely purged from the [redacted] databases until [redacted]

(U) Counterintelligence Activities

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(U) Nothing to report.

(U) Intelligence-related Activities

~~(S//SI//NF)~~ [redacted]

~~(S//SI//REL TO USA, FVEY)~~ Although not violations of E.O. 12333 and related directives, NSA/CSS reports [redacted] instances in which database access was not terminated when the need for access was no longer required. [redacted] access to FISA data was not terminated when the NSA/CSS employees transferred or forward-deployed to locations in [redacted] and [redacted] [redacted] occasions, access to PAA data was not terminated when NSA/CSS analysts deployed to [redacted] Once identified, accesses were revoked.

(b)(1)
(b)(3)-P.L. 86-36

(U) **Destruction Delays**

~~(TS//SI//NF)~~ [redacted] inadvertent intercepts collected from [redacted] were purged [redacted] but the analyst forgot to [redacted] The NSA analysis and production staff found the oversight [redacted] at which time the collection was deleted. The analyst reviewed the procedures for purging collection to lessen the possibility of a recurrence of a retention violation.

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ On [redacted] occasions, NSA/CSS analysts did not purge unintentional collection from NSA databases in a timely manner. [redacted] an email selector for a legitimate foreign target was detasked on [redacted] in the United States. Collection was not removed from the [redacted] data repositories until [redacted] the selector for a different target was detasked on [redacted] but collection was not purged from the [redacted] databases until [redacted]

2. (U//~~FOUO~~) NSA/CSS OIG Intelligence Oversight Inspections, Investigations, and Special Studies.

(U//~~FOUO~~) During this quarter, the Office of Inspector General reviewed various intelligence activities of the NSA/CSS to determine whether they had been conducted in accordance with applicable statutes, Executive Orders, Attorney General procedures, and Department of Defense and internal directives. With few exceptions, the problems uncovered were routine and showed that operating elements understand the restrictions on NSA/CSS activities.

(U//~~FOUO~~) **NSA/CSS Hawaii.** The inspection found non-compliance in the completion of initial and annual refresher intelligence oversight training and the database to track training for those with access to SIGINT databases and their auditors was not accurate. In a future report, the NSA/CSS Inspector General will update actions taken by NSA/CSS Hawaii to correct the inspection findings. A highlight of the inspection was the [redacted] database and Standard Operating Procedure (SOP) developed by [redacted] section. The SOP has reduced the detasking time from [redacted] minutes and has helped prevent collection violations.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) **NSA/CSS Colorado.** The inspection found non-compliance in the completion of initial and annual refresher intelligence oversight training. NSA/CSS Colorado lacked a process to track training for employees with access to NSA databases and had no processes to update the data. Operations employees displayed a good understanding of the intelligence oversight authorities in relation to collection, minimization and dissemination.

3. (U) Substantive Changes to the NSA/CSS Intelligence Oversight Program.

(U) Nothing to report.

4. (U) Changes to NSA/CSS published directives or policies concerning intelligence, counterintelligence, or intelligence-related activities and the reason for the changes.

(U) Nothing to report.

5. (U) Procedures governing the activities of Department of Defense (DoD) intelligence components that affect U.S. persons (DoD Directive 5240.1-R, Procedure 15) Inquiries or Matters Related to Intelligence Oversight Programs.

(U) Nothing to report.